Alta Affidabilità in Linux

Come garantire sempre e comunque i servizi erogati

Micky Del Favero - Dino Del Favero
micky@delfavero.it - dino@delfavero.it

BLUG - Belluno Linux User Group
Linux Day 2006 - Feltre 28 ottobre 2006

Ma serve?

Legge di Finangle:
Se qualcosa può andare storto allora lo farà.

Corollario:
Ogni soluzione genera nuovi problemi.

Alta Affidabilità

Garanzia sui servizi erogati.
I servizi devono continuare ad essere disponibili anche in caso di guasto alle macchine su cui girano.

Garanzia e sicurezza dei dati memorizzati.
Deve essere garantita l'integrità dei dati memorizzati sui supporti di memorizzazione di massa, e deve essere garantita la loro raggiungibilità futura anche in caso di guasti solamente alle *entità* (persone o processi) autorizzate a farlo.

Garanzia dei servizi

È necessario che i servizi siano sempre disponibili, per garantirli vi sono due possibilità (non mutualmente esclusive):

Più macchine erogano lo stesso servizio.

In caso di guasto ad una di esse il servizio è comunque garantito dalle altre.

Più macchine erogano servizi diversi.

In caso di guasto ad una di esse le altre se ne rendono conto e una (o più) viene incaricata di fornire il servizio che girava sulla macchina guasta è che così garantito.

Garanzia dei dati

Per garantire l'integrità dei dati anche in caso di guasti sono necessari:

Dischi ridondati.

In caso di guasto ad un supporto i dati non vengono persi perché duplicati su altri dischi.

Volumi ridondati.

Un volume virtuale è gestito da più volumi su macchine diverse, in caso di guasto ad una macchina i dati sono comunque garantiti essere disponibili.

Garanzia dei dati

Garantire la sicurezza dei dati richiede:

Controllo di accesso.

Attraverso un sistema di autenticazione e autorizzazione viene garantita la lettura dei dati solo alle entità autorizzate.

Cifratura dei dati.

I dati su disco devono essere cifrati in modo da garantire l'accesso solo ad entità autorizzate anche in caso di compromissione della macchina che li contiene.

Garanzia dei servizi su Linux

La garanzia dei servizi può essere ottenuta attraverso:

Linux Virtual Server

Più macchine forniscono lo stesso servizio. Un *director*, ridondato, garantisce il bilanciamento del carico sulle macchine controllando la loro raggiungibililtà.

heartbeat

Un processo che gira su ogni macchina del cluster ascolta il “battito cardiaco” delle altre e in caso di guasto esegue uno script che in genere lancia il servizio non più disponibile su un’altra macchina.

ucarp

Un processo che gira su ogni macchina del cluster controlla le altre siano raggiungibili in caso contrario esegue uno script che generalmente lancia il servizio non più disponibile su un’altra macchina.

Garanzia dei servizi su Linux

Avere un *cluster* di macchine che fornisce un servizio richiede venga mantenuto sincronizzato il filesystem su tutte le macchine:

DRBD

Data Redundancy Block Device: un dispositivo a blocchi virtuale attivo-passivo che si mantiene sincronizzato su tutte le macchine.

gfs

Global File System: un cluster filesystem che condivide un dispositivo a blocchi in modo attivo-attivo fra i nodi.

lustre

un cluster filesystem performante, scalabile (anche 10.000 nodi), flessibile e sicuro (zero SPOF).

Garanzia dei dati su Linux

Il filesystem oltre ad essere sincronizzato e consistente fra tutti i nodi deve anche essere localmente sicuro:

md

Multiple Devices un dispositivo a blocchi che implementa RAID 0-1-4-5-10 su Linux, un guasto ad un disco non pregiudica l'integrità del volume.

LVM

Logical Volume Manager un dispositivo a blocchi che implementa un sistema di volumi logici con caratteristiche avanzate: modifica dimensioni a caldo, snapshot del filesystem...

Sicurezza dei dati su Linux

L'Alta Affidabilità necessita garanzia di accesso ai dati solo ad entità autorizzate:

attributi

un sistema di attributi da affiancare ai classici permessi per limitare alcune operazioni sui file.

Posix ACL

un sistema standardizzato di permessi che garantiscono una granularità molto fine sui controlli di accesso ai file.

capabilities

un sistema per limitare la possibilità di accesso al sistema ai processi.

Sicurezza dei dati su Linux

Oltre alla sicurezza attiva serve anche la sicurezza passiva, in caso di furto non deve essere possibile avere accesso ai dati:

loop-aes

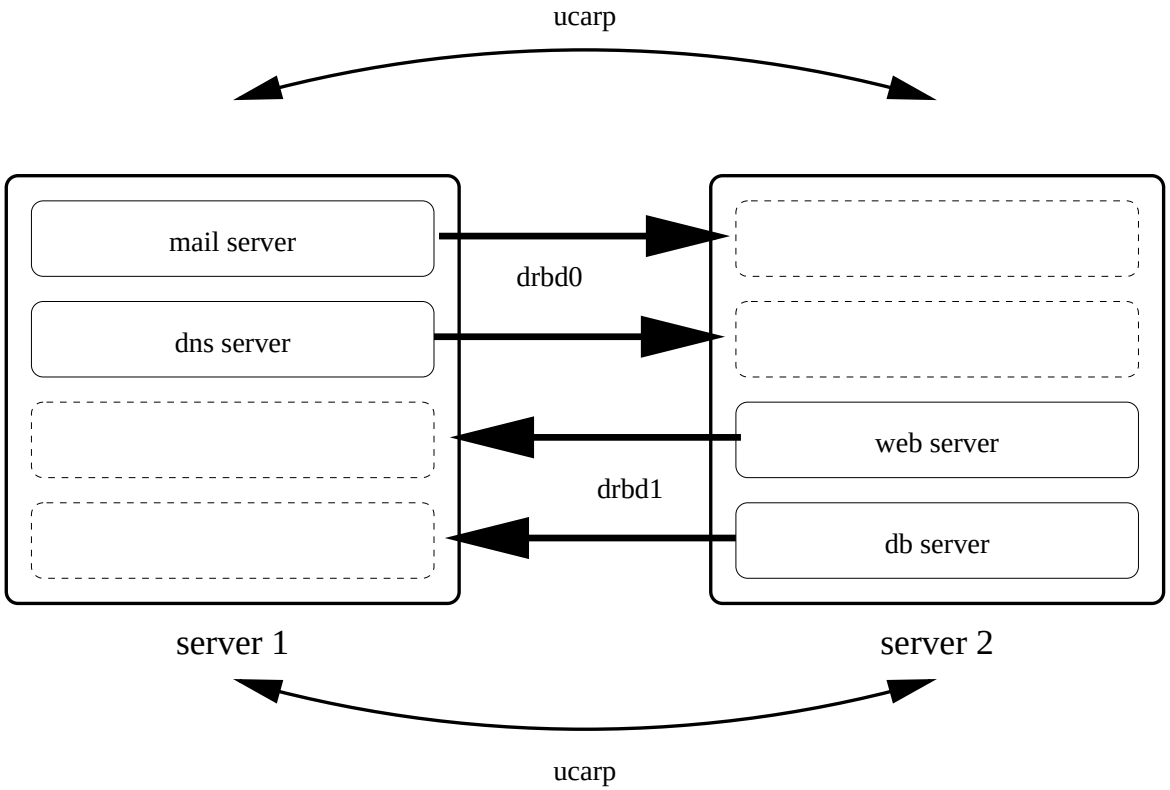
un dispositivo a blocchi che in modo trasparente cifra un dispositivo loop impendendo l'accesso ai dati ad entità non autorizzate.

dm-crypt

un dispositivo a blocchi che in modo trasparente cifra il filesystem impendendo l'accesso ai dati ad entità non autorizzate.

Un semplice esempio

DRBD + ucarp



Configurazione DRBD

drbd.conf (server1)

```
resource server1 {
  protocol C;
  on server1 {
    device     /dev/drbd0;
    disk       /dev/vg/drbd0-lv;
    address    10.222.33.1:7789;
    meta-disk  /dev/vg/md0-lv[0];
  }
  on server2 {
     # ...
  }
}
resource server2 {
  protocol C;
  # ...
}
```

Configurazione ucarp

ucarp

```
/usr/sbin/ucarp -i eth0 -s 10.21.19.10 -v 11 -p drbd0 \
    -a 10.21.19.11 -u /etc/ucarp/loc-up.sh \
    -d /etc/ucarp/loc-down.sh --shutdown --neutral --daemonize
```

/etc/ucarp/loc-up.sh

```
#!/bin/sh
/sbin/ip addr add 10.21.19.11 dev eth0
/etc/init.d/mysql start
/etc/init.d/apache2 start
```

/etc/ucarp/loc-down.sh

```
#!/bin/sh
/etc/init.d/apache2 stop
/etc/init.d/mysql stop
/sbin/ip addr del 10.21.19.11/32 dev eth0
```

Domande?

Grazie per l’attenzione.